TD d'arithmétique

Exercice 1 Montrer que la relation de divisibilité sur $\mathbb{N}$ est une relation d'ordre.

Solution. On doit montrer que la relation de divisibilité sur $\mathbb{N}$ est réflexive, antisymétrique et transitive. Réflexivité : Soit a quelconque dans $\mathbb{N}$. En écrivant $a = a \cdot 1$, on voit que a divise a. Antisymétrie : Soient $a, b \in \mathbb{N}$ tels que $a|b$ et $b|a$. Alors $b = ac$ avec $c \in \mathbb{N}$ et $a = bd$ avec $d \in \mathbb{N}$. Donc $b = (bd)c = b(dc)$, où $dc \in \mathbb{N}$, ce qui implique que $dc = 1$. Comme 1 est l'unique élément de $\mathbb{N}$ inversible dans $\mathbb{N}$, on en déduit que $d = c = 1$, donc que $a = b$. Transitivité : Soient $a, b, c \in \mathbb{N}$ tels que $a|b$ et $b|c$. Alors $b = ac$ avec $c \in \mathbb{N}$ et $c = bd$ avec $d \in \mathbb{N}$. Donc $c = (ac)d = a(cd)$, où $cd \in \mathbb{N}$, ce qui montre que $a|c$.

Exercice 2 Calculer $D(5)$, $D(6)$ et $D(8)$

Solution. On a : $D(5) = \{-5, -1, 1, 5\}$, $D(6) = \{-6, -3, -2, -1, 1, 2, 3, 6\}$ et $D(6) = \{-6, -4, -2, -1, 1, 2, 4, 8\}$.

Exercice 3 Montrer que, dans $\mathbb{Z}$, si $a|b$ et $a|c$, alors $a|(b + c)$.

Solution. Si $a|b$ et $a|c$, alors $b = aq$ avec $q \in \mathbb{Z}$ et $c = aq'$ avec $q' \in \mathbb{Z}$. Donc $b + c = aq + aq' = a(q + q')$, où $q + q' \in \mathbb{Z}$. Donc $a|(b + c)$.

Exercice 4 Montrer que, dans $\mathbb{Z}$, si $a|b$ et $b|a$, alors $a \in \{-b, b\}$.

Solution. Supposons que $a|b$ et $b|a$. Alors $b = ac$ avec $c \in \mathbb{N}$ et $a = bd$ avec $d \in \mathbb{N}$. Donc $|b| = |a||c|$ et $|a| = |b||d|$. Il s'ensuit que $|a| = |a||cd|$, et donc que $|cd| = 1$. Ceci implique que $|c| = |d| = 1$, donc que $d \in \{-1, 1\}$. L'équation $a = bd$ montre alors que $a \in \{-b, b\}$.

Exercice 5 Soient $a, b \in \mathbb{Z}$. Démontrer l'équivalence entre

(a) $D(a) = D(b)$;

(b) $a = b$ ou $a = -b$.

Solution. Supposons (a). Puisque $a \in D(a) = D(b)$, $a|b$. De même, puisque $b \in D(b) = D(a)$, $b|a$. Comme on est dans $\mathbb{Z}$, on en déduit, *via* l'exercice précédent, que $a = b$ ou $a = -b$. Réciproquement, supposons (b). Si $a = b$, il est clair que $D(a) = D(b)$. Si $a = -b$, alors $D(a) = D(-b) = D(b)$.

Exercice 6 Écrire 13 en base 2, en base 3, puis en base 7.

Solution. Commençons par la base 2. En utilisant la division euclidienne, on obtient :

$13 = 6 \times 2 + 1$, donc $q_0 = 6$ et $r_0 = 1$;

$6 = 3 \times 2 + 0$, donc $q_1 = 3$ et $r_1 = 0$;

$3 = 1 \times 2 + 1$, donc $q_2 = 1$ et $r_2 = 1$;

$1 = 0 \times 2 + 1$, donc $q_3 = 0$ et $r_3 = 1$.

Le dernier quotient non nul est donc $q_2 = 1$. On en déduit que $(13)_{10} = (1101)_2$. On vérifie en effet que $1 \times 2^0 + 0 \times 2^1 + 1 \times 2^2 + 1 \times 2^3 = 13$. En appliquant la même méthode pour les bases 3 et 7, on obtient : $(13)_{10} = (111)_3 = (16)_7$.

Exercice 7 Montrer que $10^6 = 1 (\mathrm{mod}\, 7)$.

Solution. On a $10 = 3 (\mathrm{mod}\, 7)$, donc $10^2 = 9 (\mathrm{mod}\, 7) = 2 (\mathrm{mod}\, 7)$, donc $10^6 = 2^3 (\mathrm{mod}\, 7) = 1 (\mathrm{mod}\, 7)$.

Exercice 8 Déterminer le chiffre des unités de 3^{12}.

SOLUTION. Le chiffre des unités de 3^{12} est le reste de la division euclidienne de 3^{12} par 10. On a $3 = 3 (\mathrm{mod}\, 10)$, donc $3^2 = 9 (\mathrm{mod}\, 10) = -1 (\mathrm{mod}\, 10)$, donc $3^{12} = (-1)^6 (\mathrm{mod}\, 10) = 1 (\mathrm{mod}\, 10)$. Le chiffre cherché est donc 1.

Exercice 9 Trouver le reste de la division par 13 du nombre 100^{1000}.

SOLUTION. On cherche r tel que $100^{1000} = r (\mathrm{mod}\, 13)$ et $0 \leq r < 13$. Puisque $100 = 9 + 7 \times 13$, on a : $100 \equiv 9 (\mathrm{mod}\, 13)$. Donc $100^2 \equiv 81 (\mathrm{mod}\, 13) \equiv 3 (\mathrm{mod}\, 13)$ (puisque $81 = 3 + 6 \times 13$). On obtient ensuite : $100^3 \equiv 27 (\mathrm{mod}\, 13) \equiv 1 (\mathrm{mod}\, 13)$ puis, pour tout $k \in \mathbb{N}$,

$$100^{3k} = (100^3)^k \equiv 1 (\mathrm{mod}\, 13).$$

On cherche donc s tel que $1000 = 3k + s$ (c'est-à-dire, $1000 \equiv s (\mathrm{mod}\, 3)$) et $0 \leq s < 3$. On écrit alors : $10 \equiv 1 (\mathrm{mod}\, 3)$, puis

$$1000 = 10^3 \equiv 1 (\mathrm{mod}\, 3).$$

Donc $s = 1$. Finalement, on a :

$$100^{1000} = 100^{3k+1} = 100^{3k} \times 100 \equiv (1 \times 9) (\mathrm{mod}\, 13) \equiv 9 (\mathrm{mod}\, 13).$$

Puisque $0 \leq 9 < 13$, le reste cherché est égal à 9.

Exercice 10 Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Montrer que, si $a \equiv b (\mathrm{mod}\, n)$, alors $a^n \equiv b^n (\mathrm{mod}\, n^2)$.

SOLUTION. La condition $a \equiv b (\mathrm{mod}\, n)$ peut s'écrire :

$$\exists k \in \mathbb{Z} : \quad a = b + kn.$$

Ainsi, en utilisant la formule du binôme de Newton,

$$a^n = (b + kn)^n = \sum_{p=0}^{n} C_n^p b^{n-p} k^p n^p = b^n + C_n^1 b^{n-1} kn + \sum_{p=2}^{n} C_n^p b^{n-p} k^p n^p.$$

En remarquant que $C_n^1 = n$, on obtient :

$$a^n - b^n = b^{n-1} kn^2 + \sum_{p=2}^{n} C_n^p b^{n-p} k^p n^p = \left[b^{n-1} k + \sum_{p=2}^{n} C_n^p b^{n-p} k^p n^{p-2} \right] n^2.$$

Le nombre entre crochets est entier, ce qui montre que $a^n \equiv b^n (\mathrm{mod}\, n^2)$.

Exercice 11 (1) Démontrer que le nombre $7^n + 1$ est divisible par 8 si n est impair.

(2) Dans le cas où n est pair, donner le reste de la division de $7^n + 1$ par 8.

SOLUTION.

(1) Les entiers naturels n impairs sont les entiers de la forme $n = 2k + 1$ avec $k \in \mathbb{N}$. Nous allons montrer par récurence que $8 \,|\, 7^{2k+1} + 1$ pour tout $k \in \mathbb{N}$. La propriété annoncée est vraie pour $k = 0$. Supposons qu'elle soit vraie pour un certain $k \in \mathbb{N}$, et montrons qu'elle est encore vraie pour $k + 1$. On a :

$$8 \,|\, 7^{2k+1} + 1 \quad \Longleftrightarrow \quad 7^{2k+1} + 1 \equiv 0 (\mathrm{mod}\, 8) \quad \Longleftrightarrow \quad 7^{2k+1} \equiv -1 (\mathrm{mod}\, 8).$$

Donc

$$7^{2(k+1)+1} + 1 = 7^{2k+1} \times 7^2 + 1 \equiv (-1 \times 1 + 1) (\mathrm{mod}\, 8) \equiv 0 (\mathrm{mod}\, 8),$$

où l'on a utilisé le fait que $7^2 = 49 \equiv 1 (\mathrm{mod}\, 8)$. Donc $8 \,|\, 7^{2(k+1)+1} + 1$.

(2) Puisque $7 \equiv -1 (\mathrm{mod}\, 8)$, $7^n \equiv (-1)^n (\mathrm{mod}\, 8)$. Si n est pair, on a donc $7^n \equiv 1 (\mathrm{mod}\, 8)$. Donc

$$7^n + 1 \equiv (1+1) (\mathrm{mod}\, 8) \equiv 2 (\mathrm{mod}\, 8).$$

Puisque $0 \leq 2 < 8$, on en déduit que 2 est le reste de la division de $7^n + 1$ par 8.

Exercice 12 Déterminer, en utilisant la notion de congruence, le chiffre des unités de $7^{(7^7)}$.

SOLUTION. Le chiffre des unités de $7^{(7^7)}$ est le reste de la division euclidienne de $7^{(7^7)}$ par 10. On cherche donc $R \in \{0, \ldots, 9\}$ tel que $7^{(7^7)} = R (\mathrm{mod}\, 10)$.
Posons $N = 7^7$. On a : $7^2 = 49 = -1 (\mathrm{mod}\, 10)$, donc $7^4 = 1 (\mathrm{mod}\, 10)$. Donc pour tout $q \in \mathbb{N}$, $7^{4q} = (7^4)^q = 1 (\mathrm{mod}\, 10)$. Ceci suggère, pour réduire le problème, de mettre $N = 7^7$ sous la forme $N = 4q + r$ avec $r \in \{0, \ldots, 3\}$. On aura ainsi

$$7^N = 7^{4q+r} = 7^r (\mathrm{mod}\, 10).$$

Cherchons donc r. On a :

$$7 = 3 (\mathrm{mod}\, 4) \Longrightarrow 7^2 = 9 (\mathrm{mod}\, 4) = 1 (\mathrm{mod}\, 4) \Longrightarrow 7^6 = 1 (\mathrm{mod}\, 4) \Longrightarrow 7^7 = 7 (\mathrm{mod}\, 4) = 3 (\mathrm{mod}\, 4).$$

On voit donc que $r = 3$. Finalement,

$$7^N = 7^3 (\mathrm{mod}\, 10) = (7^2 \times 7) (\mathrm{mod}\, 10) = (-1 \times 7) (\mathrm{mod}\, 10) = 3 (\mathrm{mod}\, 10).$$

Il s'ensuit que $R = 3$, c'est-à-dire, que le chiffre des unités de $7^{(7^7)}$ est 3.

Exercice 13 Montrer que quel que soit $n \in \mathbb{Z}$, 7 divise $2^{(4^n)} + 5$.

SOLUTION. On procède par récurrence. La propriété est évidemment vraie pour $n = 0$. Supposons la proprité vraie à l'ordre n, c'est-à-dire, $2^{(4^n)} + 5 = 0 |7|$, soit encore $2^{(4^n)} = 2 |7|$. Alors

$$2^{(4^{n+1})} = 2^{4^n \times 4} = (2^{4^n})^4 = 2^4 (\mathrm{mod}\, 7) = 16 (\mathrm{mod}\, 7) = 2 (\mathrm{mod}\, 7).$$

Donc $2^{(4^{n+1})} + 5 = 0 (\mathrm{mod}\, 7)$.

Exercice 14 Calculer le pgcd de 61542 et 6514.

SOLUTION. Par divisions euclidiennes successives, on obtient :

$61542 = 9 \times 6514 + 2916$;
$6514 = 2 \times 2916 + 682$;
$2916 = 4 \times 682 + 188$;
$682 = 3 \times 188 + 118$;
$188 = 1 \times 118 + 70$;
$118 = 1 \times 70 + 48$;
$70 = 1 \times 48 + 22$;
$48 = 2 \times 22 + 4$;
$22 = 5 \times 4 + 2$;
$4 = 2 \times 2 + 0$.

Le pgcd de 61542 et 6514 est le dernier reste non nul, c'est-à-dire 2.

Exercice 15 Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Démontrer que l'équation $ax \equiv b (\mathrm{mod}\, n)$ admet une solution $x \in \mathbb{Z}$ si et seulement si $a \wedge n \,|\, b$.

SOLUTION. On a :

$$ax \equiv b (\mathrm{mod}\, n) \iff \exists k \in \mathbb{N} : \; ax - b = kn.$$

Or la dernière équation s'écrit aussi $ax - kn = b$. Donc il y a équivalence entre

(i) l'équation $ax \equiv b (\mathrm{mod}\, n)$ admet une solution dans $\mathbb{Z}$;

(ii) l'équation diophantienne du premier ordre $ax + ny = b$ (d'inconnues x et y) admet une solution dans $\mathbb{Z}^2$.

D'après le cours, la condition (ii) équivaut à la condition $a \wedge n \,|\, b$.

Exercice 16 Soit X l'ensemble des nombres premiers de la forme $4k + 3$ avec $k \in \mathbb{N}$.

(1) Montrer que X est non vide.

(2) Montrer que le produit de deux nombres de la forme $4k + 1$ est encore de cette forme.

(3) On suppose que X est fini et on l'écrit alors $X = \{p_1, \ldots, p_n\}$. Soit $a = 4p_1 \times \cdots \times p_n - 1$. Montrer par l'absurde que a admet un diviseur premier de la forme $4k + 3$.

(4) Montrer que ceci est impossible et donc que X est infini.

SOLUTION.

(1) L'ensemble $X = \{p \in \mathscr{P} | \exists k \in \mathbb{N} : p = 4k + 3\}$ est non vide, puisque $3 \in X$ (prendre $k = 0$).

(2) L'assertion à montrer provient du fait que

$$(4k + 1)(4k' + 1) = 16kk' + 4k + 4k' + 1 = 4(4kk' + k + k') + 1.$$

(3) Supposons que a n'admette pas de diviseur premier de la forme $4k + 3$. Alors ses diviseurs premiers (il en existe au moins un d'après le cours) sont de la forme $4k + 1$ (puisque les nombres de la forme $4k$ et $4k + 2$ ne sont pas premiers). D'après la question(2) et le théorème fondamental de l'arithmétique (tout entier se décompose en produit de facteurs premiers), a lui-même est de la forme $4k + 1$. On a donc :

$$4p_1 \times \cdots \times p_n = a + 1 = 4k + 2, \quad \text{soit} \quad 2p_1 \times \cdots \times p_n = 2k + 1.$$

Cette dernière équation est absurde, puisque le membre de gauche est pair et le membre de droite impair. On en déduit que a admet un diviseur premier de la forme $4k + 3$, c'est-à-dire, que a est divisible par un élément p_i de X.

(4) Puisque $p_i \,|\, 4p_1 \times \cdots \times p_n$ et $p_i \,|\, a$, on a :

$$p_i \,|\, (a - 4p_1 \times \cdots \times p_n), \quad \text{c'est-à-dire} \quad p_i \,|\, 1.$$

Ceci est absurde puisque p_i est premier, et donc on a montré que X comporte une infinité d'éléments.